

### 1-3: Cómo proteger su identidad

<p><u>Elenco</u></p> <ul style="list-style-type: none"> <li>• Terri</li> <li>• Especialista en seguridad, cuarentona, negra o hispana, Antonia López</li> <li>• Víctima de robo de identidad, entre 25 y 30 años, blanca, Marsha</li> </ul> <p><u>Sinopsis</u></p> <ul style="list-style-type: none"> <li>• Terri y la especialista en seguridad se reúnen con la víctima de robo de identidad, a quien le robaron su billetera recientemente</li> <li>• Hablan sobre los tipos de robo de identidad, protecciones, qué hacer</li> </ul> <p><u>Lugar</u></p> <ul style="list-style-type: none"> <li>• Dentro de Caffeine Station, una cafetería con mucha gente, tipo Starbucks</li> </ul>	<p>A. Resumen de robo de identidad</p> <ol style="list-style-type: none"> <li>Definición de robo de identidad</li> <li>Impacto del robo de identidad</li> </ol> <p>B. Robo de identidad – bienes personales</p> <ol style="list-style-type: none"> <li>Bolsas, billeteras y monederos</li> <li>Buzón de correo</li> <li>Basura</li> <li>Cheques</li> <li>Licencia de conducir</li> </ol> <p>C. Prevención de robo de identidad con bienes personales</p> <ol style="list-style-type: none"> <li>Llevar sólo lo necesario para el día</li> <li>Proteger información clave: Número de Seguro Social, números de cuenta y tarjetas             <ol style="list-style-type: none"> <li>No los imprima en los cheques</li> <li>Uso de # alternativo en lugar de la licencia de conducir</li> <li>Destruya los estados de cuenta bancarios (tritadora de corte transversal)</li> </ol> </li> <li>Para el correo             <ol style="list-style-type: none"> <li>Buzón cerrado con llave o apartado postal</li> <li>Facturas por correo en apartados del Servicio Postal/oficinas de correos</li> <li>Depósito directo</li> </ol> </li> </ol> <p>D. Robo de identidad – electrónico y remoto</p> <ol style="list-style-type: none"> <li>En línea             <ol style="list-style-type: none"> <li>Phishing</li> <li>Pharming</li> </ol> </li> <li>Telemarketing</li> </ol> <p>E. Prevención de robo de identidad electrónico y remoto</p> <ol style="list-style-type: none"> <li>Los bancos y comerciantes legítimos no solicitan números del seguro social ni números de cuenta en línea o por teléfono             <ol style="list-style-type: none"> <li>Comuníquese con las organizaciones a través de los canales regulares para verificar</li> <li>Averigüe cómo se utilizará la información personal incluso por parte de organizaciones legítimas</li> <li>National Internet Fraud Watch Information Center, <a href="http://www.fraud.org">www.fraud.org</a>; 800-876-7060</li> </ol> </li> <li>Para computadoras             <ol style="list-style-type: none"> <li>No abra datos adjuntos desconocidos</li> <li>Firewalls</li> <li>Revisiones</li> <li>Contraseñas</li> <li>Sitio web de la Comisión Federal de Comercio en <a href="http://www.ftc.gov/infosecurity">www.ftc.gov/infosecurity</a></li> </ol> </li> <li>Revisar los estados de cuenta e informes crediticios regularmente             <ol style="list-style-type: none"> <li>Cómo obtenerlos</li> <li>Qué buscar</li> <li>Si es elegible, coloque una “alerta de servicio activo” en el informe crediticio</li> </ol> </li> </ol> <p>F. Si sospecha de robo de identidad</p> <ol style="list-style-type: none"> <li>Medidas inmediatas             <ol style="list-style-type: none"> <li>Alerta inicial de fraude</li> <li>Ordene y revise los informes crediticios</li> <li>Crear un informe de robo de identidad                 <ol style="list-style-type: none"> <li>Presentar una denuncia ante la FTC</li> <li>Presentar una denuncia ante la policía</li> </ol> </li> </ol> </li> <li>Llevar registros</li> <li>Considerar alerta de fraude extendida</li> <li>Reportar errores             <ol style="list-style-type: none"> <li>A agencias de informes crediticios</li> <li>A empresas</li> <li>A operadores de cajeros automáticos y emisores de tarjetas de débito</li> <li>A cuentas de cheques</li> <li>A emisores de tarjetas de crédito</li> </ol> </li> <li>1-877-IDTHEFT o <a href="http://www.FTC.gov/IDtheft">www.FTC.gov/IDtheft</a></li> </ol> <p>G. Excluirse del uso compartido de su información</p> <ol style="list-style-type: none"> <li>Cómo puede proteger su identidad</li> <li>Cómo excluirse</li> <li>Lo que pueden y no pueden compartir los bancos</li> <li>Avisos de privacidad</li> </ol>
--	---

*Entra tema musical aumentando de volumen.*

*Darryl está en el estudio.*

1. DARRYL: Esta es... la “Red de podcast Money Smart, con Darryl y Terri”.

*Volumen de la música baja*

2. DARRYL: Esta serie de podcasts se creó para ayudarle a conocer más sobre el dinero y la banca. Abordamos algunas de sus preguntas más urgentes y hablamos con especialistas para que las respondan y nos ayuden a entender.
3. TERRI: *(a control remoto; interrumpe)* Oye, ¿dijiste “Darryl y Terri?”
4. DARRYL: *(sonido que indica que él se apresura a apagar el micrófono de ella)* Huy. ¡Qué pena, Terri, no te escuché! Dificultades técnicas. Eeh... entonces. Hemos recibido cartas de oyentes como ustedes pidiendo consejos sobre asuntos relacionados con el dinero. Y traemos a expertos para que nos ayuden a entender los temas y contestar preguntas. *(a Terri)* ¿Terri? ¿Estás ahí?
5. TERRI: *(fingiéndose un poco molesta)* Estaba. Hasta que cerraste mi micrófono. Pero sí, estoy de vuelta.
6. DARRYL: Iba a presentar el tema.
7. TERRI: Buena idea.
8. DARRYL: Hoy comenzamos con una pregunta que recibimos de Marsha, una oyente de Eureka, California. Está preocupada por el robo de identidad. Esto es lo que dice:
9. MARSHA: *(reproducción del mensaje que dejó en el buzón de voz del programa; debe leerse de manera un poco forzada, como lo haría alguien que no es actor cuando lee algo en voz alta)* “Estimados Terri y Darryl:”
10. DARRYL: *(interrumpiendo)* Quiso decir “Darryl y Terri”.
11. MARSHA: *(continúa la reproducción)* “Hace poco me robaron mi billetera. Cancelé mis tarjetas de crédito tan pronto como me di cuenta y recibí las nuevas. ¿Es todo lo que debería haber hecho? Además, empecé a ponerme muy nerviosa por el robo de identidad. ¿Qué puedo hacer para protegerme?”
12. DARRYL: ¡Muy buenas preguntas! Para responderlas, Terri fue a la ciudad natal de Marsha en Eureka, California, con la asesora de seguridad Antonia López, una autoridad en el robo de identidad *(a Terri)* Terri, ¿estás ahí?

*Ruidos de “cafetería” en el fondo todo el tiempo. Oímos el tintineo de tazas y de vez en cuando los llamados apenas perceptibles del barista: “expreso de frambuesa, triple espuma, sin grasa, extra caliente con un toque de crema batida”, etcétera.*

13. TERRI: Ajá. Aquí sigo, Darryl. *(a los oyentes)* Visitamos a Marsha en lo que nos dicen que es uno de sus lugares de reunión favoritos: Caffeine Station. Por lo que se ve – y por lo que se oye – es también el lugar favorito de al menos la mitad de la universidad.

*Ruidos iniciales de Marsha tecleando en su computadora portátil cuando Terri y Antonia se acercan a presentarse.*

14. TERRI: Buenos días. ¿Marsha? Soy Terri, de la “Red de podcast Money Smart”.

15. MARSHA: ¡Ah, sí, cómo no, la de la radio! ¡No esperaba que vinieras!

16. TERRI: Pues aquí estoy y me acompaña una experta que responderá tus preguntas sobre el robo de identidad. ¿Tienes unos 10-15 minutos para hablar con nosotros al aire?

17. MARSHA: Eh, me tengo que ir a clase en 15 minutos...

18. TERRI: Perfecto, porque aquí tienes a la mitad de nuestro equipo de mente ágil y de habla rápida.

*Ríen*

19. TERRI: Marsha, te presento a Antonia López. Estuvo en los equipos policiales de robo de identidad en tres ciudades de Michigan e Illinois en los últimos 10 años. Trabajó con investigadores federales en algunos casos. Ahora es consultora privada y se especializa en robo de identidad.

20. MARSHA: ¡Hola!

21. ANTONIA: *(está bien si Antonia suena un poco brusca; era policía)* Es un placer.

22. TERRI: Antonia va a ayudarte y a nuestros oyentes a aprender a protegerse.

23. ANTONIA: Básicamente, lo he visto todo. Todos los trucos, todas las tácticas, lo que se te ocurra.

24. TERRI: Marsha, ¿por qué no le cuentas a Antonia lo que pasó con tu billetera?

25. MARSHA: Bueno, hace dos semanas estaba sentada, eh... *(su voz cambia ligeramente, porque estira el cuello)*...por ahí. En el sofá verde. Estaba trabajando en un ensayo. Estaba terminando mi segunda taza de café expreso, ¿o ya iba por mi primera taza de capuchino? Busqué mi billetera en el bolso, y no estaba. Busqué por todas partes. Desapareció.

26. ANTONIA: Sucede muy rápido, ¿verdad? En el futuro, mantén tu bolso sobre las piernas, no a un lado, ya que es fácil distraerse.

27. TERRI: ¿Y los hombres?

28. ANTONIA: Es más seguro llevar la cartera en un bolsillo interior de la chaqueta, o en el bolsillo delantero del pantalón; así es más difícil que un ladrón la tome.
29. ANTONIA: Me dicen que cancelaste tus tarjetas de crédito en seguida. ¿Es verdad, Marsha?
30. MARSHA: Sí. También mi tarjeta débito. Pero quien haya sido, alcanzó a cargar \$1,000 en una de mis tarjetas de débito.
31. ANTONIA: Bueno, hiciste lo correcto. Tienes que notificar a los bancos dentro de los dos días hábiles siguientes. Así, lo más que podrías tener que pagar es \$50.
32. MARSHA: ¡Vaya! Afortunadamente, no me pidieron que pagara nada. ¿Qué pasa si das aviso *después* de dos días hábiles?
33. TERRI: Podrías perder hasta \$500, o tal vez mucho más.
34. MARSHA: ¡Imposible!
35. TERRI: Pasemos al robo de identidad.
36. ANTONIA: Desde luego. Si fueron sólo tus tarjetas de crédito y la del cajero automático y las cancelaste de inmediato, eso es una cosa. Pero piensa qué más había en tu billetera. ¿Los ladrones consiguieron otra información personal de tu cartera como tu fecha de nacimiento, número del seguro social o cuenta bancaria?
37. MARSHA: No, ese día sólo llevaba mis tarjetas de crédito y algo de efectivo.
38. TERRI: ¡Qué alivio!
39. ANTONIA: Perfecto. Siempre recomiendo llevar sólo lo que uno necesita para el día. Nunca es una buena idea llevar la tarjeta del seguro social. Guárdala en casa en un lugar seguro, junto con las tarjetas de crédito que no vas a usar o en una caja de seguridad.
40. TERRI: Esa es una excelente sugerencia para Darryl cuya billetera es del tamaño de Sacramento.
41. ANTONIA: Cierto, tienes mucha suerte. Tienes que ser consciente de que esta información es de mucho valor para los ladrones. Ellos pueden usarla para abrir nuevas cuentas a tu nombre. Y ellos pueden obtenerla de cualquier lugar que se les permita, de tu bolsillo, tu cartera o incluso de tu buzón de correo. Ellos incluso revisan la basura para encontrar esta información.
42. MARSHA: ¡Puaj!
43. ANTONIA: Por eso, no imprimas tu número del seguro social en tus cheques ni lo uses en tu licencia de conducir. También ten cuidado con los estados de cuenta bancarios o cualquier documento con información personal. Eso es lo que buscan los ladrones en la basura.

44. TERRI: Saben... Creo que la chaqueta favorita de Darryl salió de un contenedor de basura. Por eso lo dejamos en el estudio. Antonia, me sugeriste que comprara una trituradora de papel.
45. ANTONIA: Sí. Es la mejor forma de deshacerse de estados de cuenta bancarios y otros papeles que tengan tu número del seguro social o de cuenta. Archívalos con seguridad si tienes que conservarlos y destrúyelos si no. Fíjate que sea una trituradora de corte transversal. Así, es casi imposible volver a unir los documentos.
46. TERRI: Para dejar de recibir muchas de esas ofertas de tarjeta de crédito, puedes “excluirte”.
47. MARSHA: ¿Qué es eso?
48. TERRI: Es pedir que te borren de la lista de correo para recibir ofertas de crédito o de seguros. Con ello, los ladrones tienen menos oportunidades para intentar abrir una tarjeta de crédito a tu nombre.
49. ANTONIA: Eso significa que tu buzón de correo será menos atractivo para los ladrones.
50. MARSHA: ¡Me parece muy bien!
51. TERRI: También es fácil. Sólo llama al 1-888-OPT-OUT (1-888-567-8688) o llena el formulario en [www.optoutprescreen.com](http://www.optoutprescreen.com).
52. ANTONIA: Marsha, el ladrón no se llevó tu licencia de conducir, ¿verdad?
53. MARSHA: Desde luego.
54. ANTONIA: Eso también es bueno. Si se la hubiera llevado, sabría dónde vives. Te recomendaría que si tu buzón no tiene candado, consigas uno o un apartado postal. Usa el depósito directo si lo ofrece tu empleador.
55. MARSHA: ¡Tuve mucha suerte!
56. TERRI: Por supuesto.
57. ANTONIA: Y... y esto me ha estado molestando desde que llegamos. (*Se oye un ruido “sordo” cuando Antonia cierra la computadora de Marsha.*) Pueden robarte tu información privada en línea si utilizas una computadora pública, publicas información que no debes en las redes sociales o respondes un mensaje falso de correo electrónico o de texto.
58. MARSHA: ¡Ay! Pero esta es mi propia computadora.
59. ANTONIA: ¿Instalaste un antivirus y un firewall para protegerla?
60. MARSHA: ¡Sí!

61. ANTONIA: ¿Y los configuraste para que se actualicen automáticamente?
62. MARSHA: Mmm, creo que no. ¡Y compro y descargo música todo el tiempo!
63. TERRI: Un problema grande es un correo electrónico o mensaje de texto falso que parece de tu banco o empresa de tarjeta de crédito, o incluso de un vendedor en línea. Por lo común dice algo como que hay un problema y necesitas verificar la información de tu cuenta, contraseña y tarjeta de crédito o tendrán que suspender tu cuenta.
64. ANTONIA: Eso es una estafa de “phishing”.
65. MARSHA: ¿Cómo pescar en inglés?
66. TERRI: No, en inglés se escribe con “PH” al principio.
67. ANTONIA: También lo hacen por teléfono. Otra estafa se llama pharming...
68. MARSHA: Déjame adivinar: eso no tiene que ver con la palabra “farm”, o granja, en inglés.
69. TERRI: Correcto. También se escribe con “PH”. No sé por qué.
70. MARSHA: Por divertirse.
71. ANTONIA: Pharming es cuando el correo electrónico te lleva a un sitio web que aparenta ser de un banco o comercio en línea que conoces.
72. MARSHA: Pero, ¿cómo saber si es real o falso? (a Terri) Lo dije con “PH”.
73. ANTONIA: Lo más importante es que ningún banco o negocio *real* pide esa información en un correo electrónico o por teléfono. No des ninguna información por teléfono o correo electrónico. No hagas clic en los enlaces, ni abras los documentos adjuntos.
74. TERRI: Si no estás segura, llama al número de atención a clientes del banco que aparece en tu tarjeta de crédito o débito y que sabes que es real. Así puedes asegurarte de que no haya problemas con tu cuenta.
75. ANTONIA: También puedes contactar al Centro Nacional de Información de Fraude en [www.fraud.org](http://www.fraud.org). Ahí puedes reportar correos electrónicos y llamadas sospechosos que piden información personal. Además, tiene excelente información.
76. TERRI: Para nuestros oyentes, ¿hay otras medidas que Marsha debería haber tomado cuando le robaron la billetera?
77. ANTONIA: Marsha, hiciste bien en reportar que te habían robado tus tarjetas de crédito. Si se hubieran llevado cheques, habrías tenido que abrir una nueva cuenta de cheques y ahorro y detener el pago de los cheques faltantes. Sería buena idea tener una nueva tarjeta del cajero y nuevas claves para tus tarjetas.

**78. MARSHA:** Hmm... ahora que lo pienso, no encontré mi licencia de conducir esta mañana... tal vez se la llevaron. Puedo conseguir un duplicado, pero... ¿Cómo sé si alguien está usando mi información?

**79. ANTONIA:** En primer lugar, si no denunciaste el robo a la policía, hazlo y guarda una copia del informe policial.

Luego, asegúrate de revisar todos tus estados de cuenta del banco y tarjeta de crédito tan pronto como puedas. Busca compras que no hiciste, o nuevas tarjetas de crédito o préstamos que no solicitaste. Si ves algo sospechoso, repórtalo inmediatamente al departamento de seguridad o fraude del banco o la empresa de tarjetas de crédito.

**80.** También puedes contactar a una empresa de verificación de cheques, que notificará a las tiendas que no acepten los cheques robados. Dos que trabajan con los consumidores son TeleCheck y Certegy.

**81. TERRI:** Encontrarás los detalles de estas empresas en la sección InfoBooth de la Red de podcast Money Smart, en [www.fdicmspodcast.com](http://www.fdicmspodcast.com).

**82. ANTONIA:** Después, examina tu reporte de crédito. Por ley, puedes obtener un reporte de crédito completo y gratuito cada doce meses de cada una de las tres principales agencias de reporte de crédito. Son Equifax, Experian y TransUnion. Puedes solicitar un informe en línea en [www.annualcreditreport.com](http://www.annualcreditreport.com).

**83. TERRI:** Esta información también está en [www.fdicmspodcast.com](http://www.fdicmspodcast.com).

**84. MARSHA:** Uf, me estoy confundiendo.

**85. ANTONIA:** Voy rápido para que puedas llegar a clase. Sólo recuerda que encontrarás información completa sobre todo esto en [www.fdic.gov](http://www.fdic.gov), dentro de la sección Consumer Protection, para que puedas leerla con calma.

**86. TERRI:** Es un buen recurso. ¿Otras preguntas, Marsha?

**87. MARSHA:** ¿Qué hago cuando me den mi reporte de crédito?

**88. ANTONIA:** Revisa si hay nuevos préstamos o cuentas de crédito que no solicitaste. Si ves algo sospechoso, comunícate con el departamento de fraudes de cualquiera de las agencias de informes crediticios. Encontrarás todos los detalles en [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft). Es conveniente que coloquen una alerta inicial de fraude en tu expediente; esa alerta durará 90 días.

**89. MARSHA:** Bueno.

**90. ANTONIA:** De hecho, para estar realmente segura, pide una alerta inicial de fraude en tu expediente incluso antes de obtener tu reporte de crédito. Esto indica a los posibles

acreedores que deben tomar medidas adicionales cuando tú, o alguien que se hace pasar por ti, intenta abrir una cuenta a tu nombre.

91. TERRI: Y también hay un alerta de fraude extendida, ¿no?
92. ANTONIA: Correcto. Marsha, eso es si llegas a ser víctima del robo de identidad. Dura siete años. Los acreedores potenciales tienen que tomar aún más medidas antes de abrir una cuenta a tu nombre.
93. TERRI: Sé que no es tu situación, Marsha, pero siempre me gusta decirle al público que si conoce a personal militar activo, debe contarles de la “alerta de servicio activo”.
94. ANTONIA: Correcto. Indica a los acreedores potenciales que tomen medidas extras al abrir cuentas para personal en servicio militar activo.
95. TERRI: Se nos acaba el tiempo... ¿Algún último consejo para Marsha?
96. ANTONIA: Mucha suerte, Marsha. Y algún día tienes que hablar o comunicarte con tus acreedores, la policía o las agencias de informes crediticios, lleva bien tus registros. Y apresúrate a dar los pasos que no hayas tomado. Puede marcar una gran diferencia para evitar problemas después.
97. MARSHA: Antonia y Terri, muchas gracias.
98. TERRI: Antonia, gracias por compartir tanta información sobre el robo de identidad.
99. ANTONIA: De nada.

*Entra tema musical aumentando de volumen*

100. TERRI: Bueno, me despido desde Caffeine Station en Eureka, California. Esto fue la “Red de podcast Money Smart, con Terri y Darryl”.
101. DARRYL: ¡Eureka! Es *Darryl* y Terri.
102. TERRI: NO puedo creer que hayas dicho eso.

*Música se va apagando*